Memorandum

Date: March 24, 2009

To: Office of the Commissioner

Attention: Commissioner J. A. Farrow

From: **DEPARTMENT OF CALIFORNIA HIGHWAY PATROL**
Office of Assistant Commissioner, Inspector General

File No.: 005.9968.A14728.010

Subject: FOLLOW-UP REVIEW OF THE 2007 FINANCIAL INTEGRITY AND STATE MANAGER'S ACCOUNTABILITY (INFORMATION SECURITY OFFICER) AUDIT

On June 8, 2007, The Office of the Commissioner directed the Office of Internal Affairs, Audits and Evaluation Unit, (reorganized under the Office of Inspections, Audits Unit) to perform an audit of the California Highway Patrol's (Department) internal control systems. This request was initiated pursuant to the Financial Integrity and State Manager's Accountability Act of 1983, the provisions are stated in Government Code Sections 13400 through 13407. The audit scope period covered fiscal years 2005/2006 and 2006/2007. However, primary testing was conducted during the later fiscal year to provide a current evaluation of internal controls.

Based on the review of the Department's accounting and administrative controls, this audit revealed the Department has multiple internal controls in place to safeguard state assets. However, although the controls are adequate, weaknesses were observed. The results of the audit were discussed in the 2007 Evaluation of Internal Accounting and Administrative Control Systems Final Report.

Follow-up related fieldwork was conducted from August 7 - 15, 2008. The objective of this follow-up review was to determine if the Department has implemented corrective actions for deficiencies noted in the 2007 Evaluation of Internal Accounting and Administrative Control Systems Final Report. The follow-up review focused on available documentation to evaluate progress.

It should be noted that the Department did not fully implement all corrective actions addressed in the 2007 Evaluation of Internal Accounting and Administrative Control Systems Final Report. As part of this follow-up review, the Office of Inspections held discussions with the parties involved concerning the specific actions taken to implement recommendations from the initial review. This was supplemented by an examination of the records.

This review disclosed the Department did not fully implement corrective actions for all findings. The Office of Inspections validated the corrective work adequately addressed one of the two

weaknesses. I acknowledge the Information Security Officer (ISO) does not report directly to the agency director as required by the State Administrative Manual (SAM), Section 4841.1. However, the Commissioner has designated me with the responsibility to oversee the Department's compliance with policies and procedures regarding the security of information assets and I report directly to the Commissioner. The reassignment of the ISO from the Assistant Commissioner, Staff (who has oversight responsibilities for information technology programs) to me mitigates the risk to the Department. Therefore, the Department has knowingly and willingly accepted the risk of not having the ISO report directly to the Commissioner in accordance with SAM, Section 4841.1.

If you have any questions, please contact Roger Ikemoto, Senior Management Auditor at (916) 451-8405.

M. C. A. SANTIAGO
Assistant Commissioner

Attachment

cc: Office of the Assistant Commissioner, Staff
Information Security Officer
Office of Inspections, Audits Unit

INFORMATION SECURITY OFFICER FOLLOW-UP REVIEW
AUGUST 2008

On December, 2007, the Office of the Commissioner sent a memorandum to the Office of the Assistant Commissioner, Staff requesting a response to the 2007 Financial Integrity and State Manager's Accountability (FISMA) Act draft audit report. The report identified two reportable audit findings to the Department's Information Management Division specifically of the Department's Information Security Officer (ISO). The memorandum also established the Audits Unit would be following-up on the 2007 FISMA audit of the ISO and requested documents based on the ISO's response to the audit findings.

This review is an assessment of the corrective actions completed, as documented in the Department's Information Technology (IT) response memorandum. Prior to the arrival of the auditor, a request for documents was submitted by the Audits Unit's auditor to the ISO. The auditor began the follow-up review on August 5, 2008.

The Audits Unit reviewed:

- Office of Inspector General Proposed Organizational Chart for the current period retained by the ISO
- Supporting documents such as copies of State Administrative Manual (SAM), Agency Management Responsibilities, PowerPoint Presentation of ISO's Roles and Responsibilities, State ISO's Typical Classifications
- Information Security Officer's job duty statement.
- FISMA (ISO) audit final report
- FISMA (ISO) audit work papers

FINDING 1: **There is no evidence showing that the Department's Information Security Officer (ISO) is directly responsible to the Department's Director (Commissioner).**

Condition: The Department's ISO reports to a lieutenant assigned to Assistant Commissioner, Staff. Additionally, IMD, which is responsible for the Department's IT functions, also reports directly to Assistant Commissioner, Staff. Since Assistant Commissioner, Staff has direct responsibility over the information processing, technology operations, and information security functions it may give the appearance of a conflict of interest.

Criterion: SAM Section 4841.1 states, "The ISO is required to oversee agency compliance with policies and procedures regarding the security of information assets. The ISO must be directly responsible to the agency director for this purpose and be of a sufficiently high-level classification that he or she can execute the responsibilities of the office in an effective and independent manner. To avoid conflicts of interest, the ISO should not

have direct responsibility for information processing, technology operations, or for agency programs that employ confidential information."

Recommendation: Recommend the Department's ISO report directly to the Commissioner or Deputy Commissioner.

Auditee Response: At the time of the audit, the functional supervision for the ISO was assigned to the administrative lieutenant who reports to the Office of Assistant Commissioner, Staff. However, to address and resolve the information security reporting issue, the ISO will interact and report directly to the Assistant Commissioner, Staff, who is part of Executive Management.

Auditor's Observation: Since IMD is an area of responsibility of Assistant Commissioner, Staff, requiring the ISO to report directly to the Assistant Commissioner, Staff, does not resolve the conflict of interest. Additionally, after the Department's reorganization, the ISO began reporting to the Assistant Commissioner, Inspector General whose responsibility does not include managing IMD. Furthermore, the Commissioner has designed the Assistant Commissioner, Inspector General with the responsibility to oversee the Department's compliance with policies and procedures regarding the security of information assets. Although this reporting structure change reduces the conflict of interest, it does not fully comply with SAM, Section 4841.1. Hence, it appears the Department has knowingly and willingly accepted the risk of not having the Department's ISO report directly to the Department's Director (Commissioner).

Auditor Conclusion: Not Implemented.

FINDING 2: **It appears that the Department's ISO position is not classified correctly.**

Condition: Currently, the ISO position is classified as supervisory; however, the ISO does not directly supervise any staff nor does staff report to the ISO.

Criteria: Government Code Section 19051 states, "No one person shall be appointed under a class not appropriate to the duties to be performed."

The State Personnel Board (SPB) has delegated to the Department and other state agencies the authority to examine, appoint, and promote civil service employees, subject to review by the SPB. With that delegation comes the responsibility on the part of the Department to ensure that all examinations conducted, and all appointments and promotions made within the Department, comport to civil service merit requirements.

Recommendation: Recommend the Department properly classify the ISO position.

Auditee response: The ISO's classification was incorrectly documented. A call to Personnel Services Section verified the position as a System Software Specialist 111 (Technical). The change has been reflected on the current organizational chart.

Auditor's Observation: The Department's organization chart lists the ISO's classification as a System Software Specialist 111 (Technical).

Auditor Conclusion: Fully Implemented.

The Department did not fully implement all corrective actions addressed in the 2007 Evaluation of Internal Accounting and Administrative Control Systems Final Report. As part of this follow-up review, the Office of Inspections held discussions with the parties involved concerning the specific actions taken to implement recommendations from the initial review. This was supplemented by an examination of the records.

The review disclosed the Department did not fully implement corrective actions for all findings. The Office of Inspections validated the corrective work adequately addressed one of the two weaknesses. We are pleased to report the Information Security Office has taken necessary actions to adequately resolve one of the two observations identified in the original 2007 Evaluation of Internal Accounting and Administrative Control Systems Final Audit Report.